IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 1:21CR226
	)	
Plaintiff,	)	JUDGE PAMELA A. BARKER
	)	
v.	)	
	)	
DAVIS LU,	)	
	)	GOVERNMENT'S OBJECTIONS TO
Defendant.	)	DEFENSE EXHIBITS

The United States of America, by and through counsel, Rebecca C. Lutzko, United States Attorney; Brian S. Deckert and Daniel J. Riedl, Assistant United States Attorneys; and Candina S. Heath, Senior Counsel, Department of Justice Computer Crime and Intellectual Property Section, files its Objections to Defense Exhibits.

Background

On the evening of July 19, 2024, counsel for the Defendant provided to the Government by email its Defendant's Exhibit List and a 162-page pdf document consisting of 104 of the 106 exhibits identified on the Defendant's Exhibit List.[1] In its email, the defense indicated that the foreign third-party company Dessault Systèmes, also known as 3DS, would be sending the defense a certification/authentication for the records referenced in Mr. Scheyer's Report,[2] which the defense indicated were included in the defense exhibits. Currently, the government objects to

[1] The Defendant's Exhibit List identifies exhibits A through BBBBB. However, exhibits II and BBBB were not included in the 162-page pdf and have not been provided since.
[2] Mr. Scheyer's Report is not identified as an exhibit on the Defendant's Exhibit List, nor included in the 162-page pdf. The government has a copy of Mr. Scheyer's Report and the PowerPoint presented by Mr. Scheyer, that were previously provided by the defense.

the defense exhibits (identified hereinafter), or anticipates objecting at trial, as being irrelevant, constituting hearsay, not the best evidence, and lacking proper foundation for admission.[3]

The defense exhibits, namely the 162-page pdf document, consists of what appear to be emails and email chains,[4] screenshots,[5] and reports.[6] The defense has only identified two defense witnesses, its retained expert Warner Scheyer and the defendant's wife. The government has no reason to believe that Mr. Scheyer or the defendant's wife will be the sponsoring witness for the authenticity or admissibility of these exhibits, as neither of them participated in any of the emails, created any of the screenshots, or authored any of reports or the documents underlying the screenshots.

Argument

I. Legal Overview

a. Relevance

Irrelevant evidence is never admissible. Fed. R. Evid. 402. Thus, the first hurdle to overcome when determining the admissibility of an exhibit is its relevance, as defined by Federal Rule of Evidence 401. Rule 401 provides that "'[r]elevant evidence' means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Evidence is relevant if it has "any tendency" to prove or disprove a "consequential" fact. Consequential facts are those that influence a jury's verdict. "A consequential fact may be something such as intent,

[3] Application of hearsay rules and Federal Rules of Evidence to exclude defendant's evidence does not violate defendant's Sixth Amendment right to present a defense. *United States v. Vasilakos*, 508 F.3d 401 (6th Cir. 2007)
[4] Defense exhibits constituting emails and email chains are A, C-E, H-M, O-Z, and JJ.
[5] Defense exhibits constituting screenshots include AA, DD-HH, KK-VV, XX-KKK, MMM, AAAA-EEEE, LLLL-BBBBB.
[6] Defense exhibits constituting reports – not from government reports or government expert witness statements – include B, G, N, BB-CC, WW.

knowledge or motive." *United States v. Marlinga*, 457 F.Supp.2d 769, 775 (E.D. Mich. 2006). Relevant evidence should be excluded if not properly authenticated. *United States v. Daneshvar*, 925 F.3d 766, 776 (6th Cir. 2019) (an email deemed relevant was inadmissible under the business record and residual hearsay exceptions).[7]

b. Authenticity

"To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). A proponent must present "sufficient proof ... that a reasonable juror could find in favor of authenticity." *United States v. Jones*, 107 F.3d 1147, 1150 n.1 (6th Cir. 1997) (citation omitted). While authentication is a "relatively low[ ] hurdle," *United States v. Farrad*, 895 F.3d 859, 878 (6th Cir. 2018), it still must be established. *United States v. Crosgrove*, 637 F.3d 646, 658 (6th Cir. 2011). Generally, the Federal Rules of Evidence 901 and 902 set out the parameters of how to authenticate evidence or provide evidence of self-authentication. The defense has not identified the means by which it intends to authenticate its exhibits, save for approximately 15 exhibits for which the government assumes the defense will attempt to authenticate via a business records certificate.

c. Hearsay

Federal Rule of Evidence 801(c) provides that "[h]earsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Per Fed. R. Evid. 801(a), a "'[s]tatement' means a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion." The

[7] If the defense argues that the residual exception applies, in part because the main purpose behind the rule is to preserve a defendant's right to confront his accusers, which is not at issue when the defendant is attempting to introduce the hearsay, the government contends that the defense is not entitled to more liberal exceptions to the hearsay rule. *United States v. Winters*, 33 F.3d 720 (6th Cir. 1994)

rules of evidence do not define an "assertion," but courts have held that "the term has the connotation of a positive declaration," *United States v. Lewis*, 902 F.2d 1176, 1179 (5th Cir. 1990) and "utterances [that] assert facts." *United States v. Gibson*, 675 F.2d 825, 834 (6th Cir.1982). So, to be hearsay, the information must be an out of court statement, by a person, and intended by the person to be a positive declaration or an expression of fact, condition or opinion. Hearsay is considered unreliable because (1) by definition, hearsay statements cannot be effectively cross-examined to test perception, memory, bias, character and so on; (2) hearsay statements are not made under oath; and (3) the trier of fact--judge or jury--cannot observe the declarant's demeanor to determine credibility.

II. Defense Exhibits

a. Emails and Email Chains

Pursuant to Fed. R. Evid. 901, the defense will have to provide authenticating testimony by someone with personal knowledge of the communication, such as the author or the recipient, or someone familiar with the "appearance, contents, substance, internal pattens, or other distinctive characteristics of the item, taken together with all the circumstances," to authenticate these documents. *United States v. Bertram*, 259 F.Supp.3d 638, 640 (E.D. KY. 2017). In addition, many of the defendant's exhibits in this case are email chains that were forwarded or replied to multiple times. Each time an email is quoted in a "reply" or "forward," the author has an opportunity to edit any part of the message they wish, including the quoted text of other portions of the chain from other senders. Consequently, the Court must direct the defense to establish the authenticity of each portion of each email chain in order to introduce any portion of the document at trial. *New York v. Microsoft Corp.,* No. Civ A. 98-1233, 2002 WL 649951, at *5 (D.D.C. 2002) (holding that the requisite foundation must be established for each portion of a

forwarded email chain for the purposes of the business records exception). Even if one or more of the emails or email chains are somehow wholly authenticated, they are still inadmissible if they are offered for the truth of the matter asserted *and* do not fall under a recognized exception to the hearsay rule. See *Bouriez v. Carnegie Mellon University*, 2005 WL 2106582, at *7 (W.D. Pa. 2005) ("Although a document is authenticated, the statements contained within the documents may be inadmissible due to the application of the rule which prohibits the use of hearsay evidence.").

A number of the email or email chain exhibits, such as defendant's exhibits C-E, L, Q, S, and X, do not include (or portions of the chain do not include) any potential testifying defense or government witness. Without a sponsoring witness, these exhibits become highly problematic as to their authenticity, relevance, and anticipated lack of a proper foundation. These exhibits further present a double hearsay concern, since the trier of fact has to rely on the proposition that the person forwarding each email relayed the information without any alterations. See *Microsoft*, 2002 WL 649951, at *5; *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 572 (D. Md. 2007).

b. Dessault Systèmes Data

No certificates of authenticity were received for the 106 proposed defense exhibits, however the defense represented that the foreign third-party company Dessault Systèmes (3DS) would be providing the defense with a "certification/authentication for the records." The Government presumes this will be a sworn-to business records certification. As best as can be determined, the defense exhibits reflecting some indicia of originating from 3DS are exhibits DD-EE, JJ-KK, PP, YY, AAA, CCC-DDD, FFF-GGG, JJJ-KKK, MMM, and TTTT.

To be properly authenticated, a foreign business record certificate must comply with 18 U.S.C. § 3505, which is similar in its requirements to Fed. R. Evid. 902(11) (which applies to authentication of domestically kept records). Assuming the certification meets the required standards, emails are "not a business record for purposes of the relevant hearsay exception simply because it was sent between two employees in a company or because employees regularly conduct business through emails; such evidence alone is insufficient to show that the email is a record, made as 'a regular practice' of the company, Fed. R. Evid. 803(6)(C), and that 'the record was kept in the course of a regularly conducted activity of a business'" *Daneshvar*, 925 F.3d at 777; Fed. R. Evid. 803(6)(B). If every single email in a company's email server constituted a business record, it would "obviate the entire purpose of the business records exception," that being, to authenticate those records regularly created in and for the normal course of business. *Id.* Among the proposed 3DS defense exhibits, JJ is an example of such an email. Additionally, randomly written or typed notes or communications do not magically become business records simply because they were authored by or in the possession of a company employee, especially if the identity of that employee, the date, or the purpose of the note or communication is unknown.

Defense exhibits PP, CCC, and MMM appear to be screenshots of electronic data combined with "notes or comments" from an unidentified person. Defense exhibit KKK appears to be a "note or comment" from an unidentified person. Defense exhibit TTTT seems to be an undated screenshot from a website, with nothing on its face to indicate that it was produced by 3DS. Even a business records certification cannot overcome the double hearsay inherent in these unidentified "notes or comments."

Finally, the defense cannot introduce any of the 3DS data through its own expert, on a surrogate or substitute expert theory. The Supreme Court in *Smith v. Arizona*, No. 22–899, 602

U.S. ___, (Argued Jan. 10, 2024-Decided June 21, 2024), held that a party, through its testifying expert, "may not introduce the testimonial out-of-court statement" of a non-testifying expert, as the basis for the testifying expert's opinion.

c. Digital Data

Some of the defense exhibits, even those that appear to originate from 3DS, are images or screenshots of digital data. Authenticating digital data requires either the testimony from a witness with personal knowledge of the system producing the data, or the proponent must establish that the data was "generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12)." *United States v. Foster*, 2024 WL 184003, *2 (N.D. Ohio 2024) (quoting Fed. R. Evid. 902(13)). Defense exhibits that appear to include such an image or screenshot include FF-HH,[8] LL-TT, VV, XX-CCC, EEE, GGG-JJJ, MMM, ZZZ-AAAA, CCCCC-EEEE, LLLL-SSSS, UUUU-XXXX, ZZZZ-BBBB. The government objects to any offer to admit these exhibits without first properly authenticating each.

The defense cannot claim authentication of an item simply because the government produced the data in discovery, or that the data was obtained in response to a subpoena. *Jonathan Pepper Co. v. Hartford Cas. Ins. Co*., 520 F. Supp. 2d 977, 981 (N.D. Ill. 2007) (argument that documents are "automatically authenticated" if a third-party produces them in response to a subpoena "defies logic").

[8] Defense exhibit HH also contains what appears to be a "comment" added to the screenshot, with an assertion of "Not Working" in bold red text. Without authentication and an exception to the hearsay rule, this comment is inadmissible (assuming that the screenshot or image itself is authenticated and admissible).

d. Evidence of Disparate Events

Defense exhibits A – L, N, Q, S, Z, and AA are, in whole or in part, related to a separate investigation prompted by a complaint initiated by the defendant *after* his employer, Eaton, suspended him for the commission of the criminal conduct alleged in the indictment. This complaint involved the defendant's claim that he received a notice in his personal Hotmail account, *after his suspension*, that an unauthorized person accessed his account on the online platform Assembla,[9] from the laptop he surrendered to Eaton. No data was found on the Defendant's Assembla site and the Government does not intend to make any mention of Assembla during the trial of this matter. These defense exhibits consist of the notice from Assembla, a report regarding the claim, and emails between various Eaton employees discussing the defendant's allegation. This matter is unrelated to the charges in the indictment and the Government intends to object to any evidence regarding the Defendant's claim as irrelevant. Further, if the defense seeks to promote this disparate event as somehow exculpating himself from the current charges, he is not permitted to elicit his own exculpatory statements through such evidence or the testimony of another witness. Such exculpatory statements are clearly inadmissible hearsay. *United States v. McDaniel*, 398 F.3d 540 (6th Cir. 2005).

Another disparate evidentiary item is defense exhibit U. This exhibit is an email chain which does not involve the defendant or any of the facts in the instant case, but instead relates to an entirely different and irrelevant investigation in Canada regarding a former Eaton employee who was alleged to have stolen proprietary data. This email is hearsay and irrelevant to the current charges. The government opposes the introduction of any such disparate evidence, or testimony involving the substance of the disparate event.

[9] Per https://get.assembla.com/, Assembla is source code and project management platform.

Conclusion

At the appropriate time during trial, the government requests that this court consider the arguments herein and exclude the above identified exhibits as irrelevant, unauthenticated, and inadmissible pursuant to federal law.

Respectfully submitted this the 21st day of July 2024.

Respectfully submitted,

REBECCA C. LUTZKO
United States Attorney

By: */s/ Brian S. Deckert*
Brian S. Deckert (OH: 0071220)
Daniel J. Riedl (OH: 0076798)
Assistant United States Attorneys
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3873/3669
(216) 522-8355 (facsimile)
Brian.Deckert@usdoj.gov
Daniel.Riedl@usdoj.gov

By: */s/ Candina S. Heath*
Candina S. Heath (TX #09347450)
Senior Counsel
U.S. Department of Justice Criminal Division
Computer Crime & Intellectual Property
John C. Keeney Building, Suite 600
Washington, DC 20530
(202) 923-5211
Email: Candina.Heath2@usdoj.gov